BUILDING BLOCK

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

MOBILE DEVICE SECURITY: CLOUD & HYBRID BUILDS

The National Cybersecurity Center of Excellence (NCCoE) is addressing the challenge of mobile device security for enterprises through collaborative efforts with industry and the information technology (IT) community, including vendors of cybersecurity solutions. This sheet provides an overview of the mobile device security project description, including background and challenge, goals, and proposed solution. For more information about the project, see recent work in mobile device security on the NCCoE website. The solution we propose is not meant to be authoritative; there may be other solutions in this fast-moving cybersecurity technology market. If you would like to propose an alternative architecture or learn about products that might be applicable to the challenge of securing mobile devices, please contact us at mobile-nccoe@nist.gov.

BACKGROUND

Mobile devices allow employees to access information resources wherever they are, whenever they need. The constant internet access available through a mobile device's cellular and Wi-Fi connections has the potential to make business practices more efficient and effective. And as mobile technologies mature, employees increasingly want to use mobile devices to access corporate enterprise services, data, and other resources to perform work-related activities.

THE CHALLENGE

If sensitive data is stored on a poorly secured mobile device that is lost or stolen, an attacker may be able to gain unauthorized access to that data. Even worse, a mobile device with remote access to sensitive organizational data could be leveraged by an attacker to gain access to that data, and any other data that user is allowed to access from that mobile device.

The challenge lies in ensuring the confidentiality, integrity, and availability of the information that a mobile device accesses, stores, and processes. Despite the security risks posed by today's mobile devices, enterprises are under pressure to employ them for several business reasons, including anticipated cost savings and employees' need to work in remote locations.

GOAL

The goal of this building block effort is to develop an approach that can be adopted by organizations across business sectors. The proposed solution will be easily configured and allow personally or enterprise-owned mobile devices to be provisioned into an enterprise mobility management system.

THE SOLUTION

The Mobile Device Security Practice Guide demonstrates how businesses can use commercially available technologies to implement an enterprise mobility management system. The system can enable secure access to the organization's sensitive email, contacts, and calendar information from users' mobile devices. These technologies enable users to work inside and outside the corporate network with a securely configured mobile device while minimizing the impact on the user experience.

BENEFITS

The proposed NCCoE mobile device security solution:

- provides users with enterprise-class protection, against both malicious applications, and loss of personal data when a device is stolen or misplaced
- provides mitigating mechanisms to reduce adverse effects on an organization if a device is compromised
- reduces capital investment by embracing modern enterprise mobility models
- facilitates multiple mobile device usage scenarios such as bring your own device (BYOD) and corporately owned personally enabled (COPE)

The National Cybersecurity Center of Excellence at the National Institute of Standards and Technology addresses businesses' most pressing cybersecurity problems with practical, standards-based solutions using commercially available technologies. The NCCoE collaborates with industry, academic, and government experts to build modular, open, end-to-end reference designs that are broadly applicable and repeatable.

LEARN MORE ABOUT NCCOE
Visit http://nccoe.nist.gov

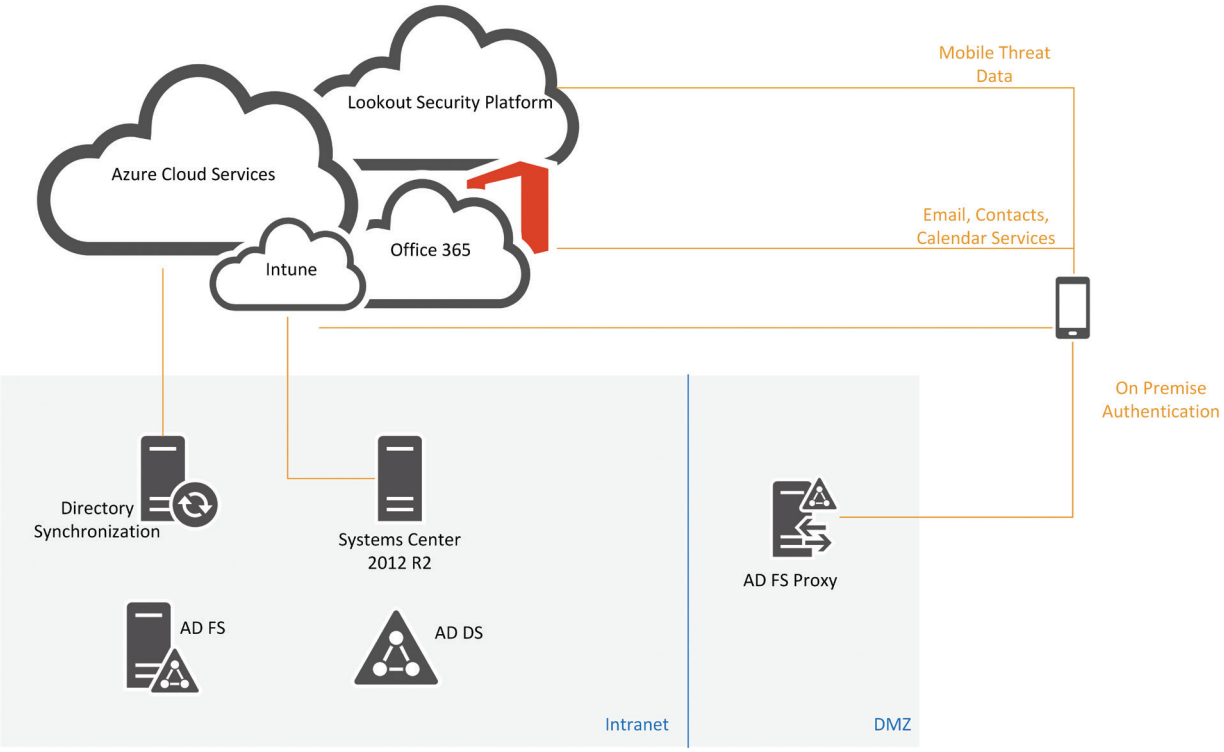
CONTACT US
nccoe@nist.gov
301-975-0200

- provides visibility for system administrators into mobile security events, quickly providing notification and identification of a compromised device
- implements industry standard mobile security controls, reducing long term costs and decreasing the risk of vendor lock-in

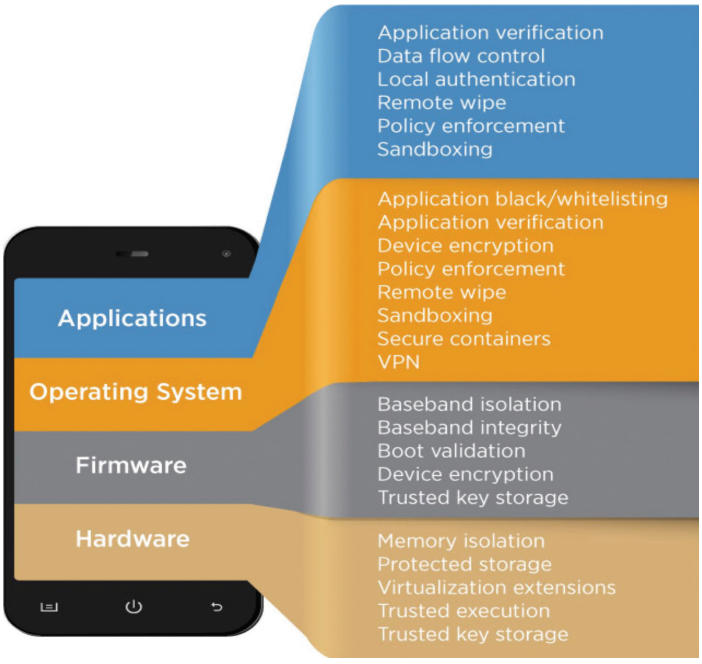
ARCHITECTURE

The NCCoE mobile device security solution allows employees to access enterprise resources and enterprise managers to push policies to mobile devices.

- mobile devices are enrolled in the enterprise mobility management system.
- enterprise management defines a set of policies, such as the requirement to use an 8-digit passcode.
- policies are pushed to mobile devices through email or some other communications channel.
- policies are enforced on the devices through an enforcement mechanism, such as the operating system or a mobile application



These processes and technologies enable users to work inside and outside the corporate network using a securely configured mobile device with security capabilities such as those shown in the figure to the right.



HOW TO PARTICIPATE

We are always seeking collaborators, insights, and expertise from businesses, the public, and technology vendors. If you are interested in contributing or collaborating on the NCCoE mobile device security project, please contact us at: mobile-nccoe@nist.gov. For more information on this project, visithttps://nccoe.nist.gov/projects/building_blocks/mobile_device_security